HKUST – Department of Computer Science and Engineering
COMP170: Discrete Math Tools for CS – Spring 2011

#	LS

Final Examination

Date: Thursday May 26, 2010 Time: 12:30- 15:00

Venue: Sports Hall

Name: _____	Student ID: _____
Email: _____	Lecture and Tutorial: _____

Instructions

- This is a closed book examination. It consists of 16 pages and 9 questions.
- Please write your name, student ID, email, lecture and tutorial sections on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page (and sometimes has an extra page for you to do work on). This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- Only use notation given in class. Do not use notation that you have learnt outside of this class that is nonstandard.
- Calculators may be used for the examination.

Questions	1	2	3	4	5	6	7	8	9	Total
Points	10	10	13	14	10	8	8	12	15	100
Score										

Student ID: _____

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Student ID: _____

Problem 1: (10 Points)

In this question, n and j are two non-negative integers such that $n = 3^j$.

A bag of n candies are distributed among a group of n children as follows:

- At the beginning, the whole bag is given to one child.
- After a child receives a bag of candies,
  - He keeps the whole bag to himself if the bag contains fewer than 3 candies;
  - Otherwise, he divides it into three smaller bags, each with 1/3 of the candies. He keeps one of the smaller bags to himself (even though it might contain 3 or more candies), and passes the other two bags to two other children who have not received any candies.

There is only one table where a bag of candies can be divided into smaller bags, and only one child can use it at one time. That means that no two children can use the table simultaneously. Suppose it takes $\log_3 m$ seconds to divide a bag of m candies into three equal size smaller bags. Furthermore, there is no idle time once the distribution process is started.

Let $T(n)$ be the number seconds it takes to distribute n candies. Find the recurrence relation and the base case value for $T(n)$. Solve the recurrence to get a closed-form solution.

For this question, your answers cannot contain the summation ($\sum$) symbol or dotted sums $(+ \ldots +)$. You might need the following equation where m is a positive integer and $x \neq 1$:

$$\sum_{i=1}^{m} ix^i = \frac{mx^{m+2} - (m+1)x^{m+1} + x}{(1-x)^2}.$$

Solution of P1: The recurrence relation is:

$$\begin{aligned} T(1) &= 0 \\ T(n) &= 2T(n/3) + \log_3 n \end{aligned}$$

Note that $n = 3^j$. Iterating the recurrence, we get

$$\begin{aligned} T(3^j) &= 2T(3^{j-1}) + j \\ &= 2[2T(3^{j-2}) + (j-1)] + j \\ &= 2^2 T(3^{j-2}) + 2(j-1) + j \\ &\vdots \\ &= 2^j T(1) + 2^{j-1}[j-(j-1)] + \ldots + 2(j-1) + j \\ &= 2^j [\frac{1}{2} + \ldots + (j-1)(\frac{1}{2})^{j-1} + j(\frac{1}{2})^j] \\ &= 2^j \frac{j(\frac{1}{2})^{j+2} - (j+1)(\frac{1}{2})^{j+1} + \frac{1}{2}}{(\frac{1}{2})^2} \\ &= 2^{j+1} - j - 2. \end{aligned}$$

Problem 2: (10 Points)

This is a continuation of the previous question. After the distribution process is completed, the children eat the candies. If a child has a bag that contains only one candy, he eats the candy himself. If a child has a bag that contains more than one candy, he shares the candies with another child who neither has his own bag of candies nor shares candies with anyone else. The two of them eat all the candies in the bag.

Consider the number of children who have candies to eat. We regard the number as a function of j instead of n. (Recall that $n = 3^j$.) Denote the number by $K(j)$. Find the recurrence relation and the base case value for $K(j)$. Solve the recurrence to get a closed-form solution.

For this question, your answers cannot contain the summation ($\sum$) symbol or dotted sums $(+\ldots+)$. You might need the following equation where m is a positive integer and $x \neq 1$:

$$\sum_{i=0}^{m-1} x^i = \frac{1-x^m}{1-x}.$$

Solution of P2: The recurrence relation is:

$$\begin{aligned} K(0) &= 1 \\ K(1) &= 3 \\ K(j) &= 2K(j-1)+2 \quad \text{for } j > 1 \end{aligned}$$

The solution of the recurrence is:

$$\begin{aligned} K(j) &= 2K(j-1)+2 \\ &= 2(2K(j-2)+2)+2 \\ &= 2^2K(j-2)+2^2+2 \\ &\vdots \\ &= 2^{j-1}K(j-(j-1))+2^{j-1}+2^{j-2}\cdots+2^2+2^1 \\ &= 3\cdot 2^{j-1}+\sum_{i=0}^{j-1} 2^i - 1 \\ &= 3\cdot 2^{j-1}+\frac{2^j-1}{2-1}-1 \\ &= 5\cdot 2^{j-1}-2 \end{aligned}$$

Problem 3: (13 Points)

For this problem, you may assume that n is a non-negative power of 6. Recall that if $f(n)$ and $g(n)$ are functions, to prove that $f(n) = O(g(n))$, you must prove that there exist some $n_0 \geq 0$ and $c > 0$ such that

$$\forall n > n_0, \quad f(n) \leq cg(n).$$

Suppose function $T(n)$ satisfies $T(1) = 10$ and, for $n > 1$

$$T(n) \leq 12T\left(\frac{n}{6}\right) + n.$$

Prove by induction that $T(n) = O(n^2)$.

Solution of P3: Prove $T(n) = O(n^2)$ is equivalent to prove there exist $n_0 \geq 0$ and $c > 0$ such that

$$\forall n > n_0, \quad T(n) \leq cn^2.$$

Base case: If we pick $n_0 = 0$, then the base case is (n = 1). In the case, we have

$$T(1) = 10 \leq c \cdot 1^2 \text{ if we pick } c \text{ to satisfy } c \geq 10.$$

Inductive Step: Assume that the statement $T(n) \leq cn^2$ is correct for $n = 6^j$, $j = 0, 1, 2, \cdots, i-1$.
When $n = 6^i$, we use the inductive hypothesis to get

$$\begin{aligned} T(n) &\leq 12T(n/6) + n \\ &\leq 12c(\frac{n}{6})^2 + n \\ &= 12\frac{cn^2}{36} + n \\ &= \frac{cn^2}{3} + n \\ &= cn^2 - \frac{2cn^2}{3} + n \\ &= cn^2 + n(1 - \frac{2cn}{3}) \\ &\leq cn^2 \quad \text{if we pick } c \text{ to satisfy } c \geq \tfrac{3}{2} \end{aligned}$$

In summary, the induction proof follows throw if we pick $n_0 = 0$ and $c \geq \max\{10, 3/2\} = 10$.

Consequently, we can conclude that $\forall n > n_0, T(n) \leq cn^2$ when $c \geq 10$ and $n_0 \geq 0$. This implies $T(n) = O(n^2)$.

Problem 4: (14 Points) Consider a game where one repeatedly throws a fair die until the total number of dots in all the throws reaches or exceeds 3. This means that if one gets 3, 4, 5, or 6 at the first throw, one stops right away. If one gets 1 or 2 at the first throw, however, one must continue.

(a) Describe the sample space for the game by listing all the possible outcomes. Here are two examples: The outcome "12" means that one gets 1 at the first throw and 2 at the second throw, and then the game is over. The outcome "113" means that one gets 1 at the first throw, 1 at the second throw and 3 at the third throw, and then the game is over.

(b) Give the probability weight for each possible outcome.

(c) Let X be the number of times one gets an odd number of dots during the game. What are the possible values of X? For the two outcomes "12" and "113", the values of X are 1 and 3 respectively.

(d) For each possible value x of X, describe the event "$X = x$".
Recall that an event is a *subset of the sample space*. To answer this question you need to give the subset of the sample space corresponding to each value of x.

(e) For all possible values x, give the probability that "$X = x$".

(f) What is $E(X)$?

(g) What is $V(X)$?

Solution of P4: (a) All possible outcomes are:
{"3","4","5","6","12","13","14","15","16","21","22","23","24","25","26", "111","112","113","114","115","116"}
i.e. There are 21 possible outcomes.

(b) For {"3","4","5","6"}, the probability of each of these outcome is $1/6$.
For {"12","13","14","15","16","21","22","23","24","25","26"}, the probability of each of these outcome is $(1/6)^2$.
For {"111","112","113","114","115","116"}, the probability of each of these outcome is $(1/6)^3$.

(c) The possible values are $0, 1, 2, 3$.

(d) The event of $X = 0$ includes the following subsets: {"22", "24", "26", "4", "6"}
The event of $X = 1$ includes the following subsets: {"3", "5", "12", "14", "16", "21", "23", "25"}
The event of $X = 2$ includes the following subsets: {"112", "114", "116", "13", "15"}
The event of $X = 3$ includes the following subsets: {"111", "113", "115"}

(e)

$$\begin{aligned}
P(X=0) &= 2\cdot\frac{1}{6}+3\cdot(\frac{1}{6})^2=\frac{5}{12},\\
P(X=1) &= 2\cdot\frac{1}{6}+6\cdot(\frac{1}{6})^2=\frac{1}{2},\\
P(X=2) &= 2\cdot(\frac{1}{6})^2+3\cdot(\frac{1}{6})^3=\frac{5}{72},\\
P(X=3) &= 3\cdot(\frac{1}{6})^3=\frac{1}{72}.
\end{aligned}$$

(f) $E(X)=0\cdot\frac{5}{12}+1\cdot\frac{1}{2}+2\cdot\frac{5}{72}+3\cdot\frac{1}{72}=\frac{49}{72}$

(g)

$$\begin{aligned}
V(X) &= E((X-E(X))^2)\\
&= (0-\frac{49}{72})^2\cdot\frac{5}{12}+(1-\frac{49}{72})^2\cdot\frac{1}{2}+(2-\frac{49}{72})^2\cdot\frac{5}{72}+(3-\frac{49}{72})^2\cdot\frac{1}{72}\\
&= \frac{2401}{5184}\cdot\frac{5}{12}+\frac{529}{5184}\cdot\frac{1}{2}+\frac{9025}{5184}\cdot\frac{5}{72}+\frac{27889}{5184}\cdot\frac{1}{72}\\
&= \frac{2401}{5184}\cdot\frac{30}{72}+\frac{529}{5184}\cdot\frac{36}{72}+\frac{9025}{5184}\cdot\frac{5}{72}+\frac{27889}{5184}\cdot\frac{1}{72}\\
&= \frac{2401\cdot 30+529\cdot 36+9025\cdot 5+27889}{5184\cdot 72}\\
&= \frac{164088}{373248}=\frac{2279}{5184}
\end{aligned}$$

Problem 5: (10 Points)
Two coins are placed in a bag. One of them is a fair coin, while the other is a special coin with tails on both sides. One of the coins is picked from the bag at random and **this** coin is tossed 2 times. Let A_i $(i = 1, 2)$ be the event that the coin comes up tail on the i-th toss.

(a) Calculate $P(A_1)$ and $P(A_2)$.

(b) Calculate $P(A_2|A_1)$.

(c) Calculate $P(A_2 \cup A_1)$.

(d) Are A_1 and A_2 independent? Why?

Solution of P5: (a) Let K be the event that the coin picked is the fair coin, and $\bar{K}$ be the event that he coin picked is the magic coin. Then,

$$P(A_1) = P(K)P(A_1|K) + P(\bar{K})P(A_1|\bar{K}) = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot 1 = \frac{3}{4}$$

Similarly, $P(A_2) = \frac{3}{4}$

(b)

$$\begin{aligned} P(A_2|A_1) &= \frac{P(A_2 \cap A_1)}{P(A_1)} \\ &= \frac{\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot 1 \cdot 1}{\frac{3}{4}} \\ &= \frac{\frac{1}{8} + \frac{1}{2}}{\frac{3}{4}} \\ &= \frac{\frac{5}{8}}{\frac{3}{4}} \\ &= \frac{5}{6} \end{aligned}$$

(c)

$$\begin{aligned} P(A_2 \cup A_1) &= P(A_1) + P(A_2) - P(A_1 \cap A_2) \\ &= \frac{3}{4} + \frac{3}{4} - \frac{5}{8} \\ &= \frac{12}{8} - \frac{5}{8} \\ &= \frac{7}{8} \end{aligned}$$

(d) No, A_1 and A_2 are not independent because $P(A_2|A_1) \neq P(A_2)$.

Problem 6: (8 Points)

Let n be a positive integer and X be a random variable that is uniformly distributed over the set $Z_n = \{0, 1, \ldots, n-1\}$. This means that $P(X = i) = \frac{1}{n}$ for any $i \in Z_n$.

Further let a and b be two other positive integers. Consider the following event E: $aX + b = 0 \bmod n$.

(a) What is $P(E)$ when $a = 2$, $b = 7$ and $n = 17$?

(b) What is $P(E)$ when $a = 3$, $b = 12$ and $n = 33$?

Explain your answers.

Solution of P6:

(a) $E : 2X + 7 = 0 \bmod 17$
The value of X is in the range [0,16]
So $2X + 7$ is in the range [7,39]
$2X + 7 = 17k$ for some integer k only when $X = 5$
Therefore $P(E) = \frac{1}{17}$

(b) $E : 3X + 12 = 0 \bmod 33$
The value of X is in the range [0,32]
So $3X + 12$ is in the range [12,108]
$3X + 12 = 33k$ for some integer k only when $X = 7$ or 18 or 29
Therefore $P(E) = 3 \cdot \frac{1}{33} = \frac{1}{11}$

Problem 7: (8 Points)

Time is continuous. In this question, suppose the time line is discretized into intervals, with the length of each interval being 1 second.

A web server has probability p $(0 < p < 1)$ of getting 1 visit in each time interval and $1 - p$ probability of getting 0 visit.

(a) How long is the server expected to wait until it gets 100 visits?

(b) How many visits is the server expected to get during 1 hour?

Explain your answers.

Solution of P7: (a) Let X_i be the number of seconds the server waits until it gets the i-th visit after $(i-1)$ visits.
This is a geometric random variable, so $E(X_i) = \frac{1}{p}$. The number of seconds for which the server is expected to wait until it gets the 100-th visit is then

$$\sum_{i=1}^{100} E(X_i) = 100 \cdot \frac{1}{p} = \frac{100}{p}$$

(b) Let Y_i be the number of visits that the server gets at the i-th second. It can be 0 or 1, and $E(Y_i) = p$.

There are 3600 seconds in one hour. So, the expected number of visits during an hour is:

$$E(\sum_{i=1}^{3600} Y_i) = \sum_{i=1}^{3600} E(Y_i) = \sum_{i=1}^{3600} p = 3600p.$$

Problem 8: (12 Points)
Consider the following simplified version of the RSA algorithm for public cryptography:

(i) Bob's public key is a pair (n, e), where n is a large prime number and e is a positive integer that is smaller than n and is relatively prime with $n - 1$.

(ii) Bob's public key is $d = e^{-1} \bmod (n - 1)$.

(iii) Alice encrypts a message m $(0 < m < n - 1)$ by calculating $c = m^e \bmod n$, and sends the ciphertext c to Bob.

(iv) Bob decrypts the ciphertext c by calculating $c^d \bmod n$.

Answer the following questions:

(a) Can Bob get back the original message? Prove your answer.

(b) Is the system secure? Explain why.

Solution of P8: (a) $d = e^{-1} \bmod (n - 1)$
Then, $ed \bmod (n - 1) = 1$
Let $ed = 1 + (n - 1)k$ for some integer k
$m^{ed} \bmod n = m^{1+(n-1)k} \bmod n = m \cdot (m^k)^{n-1} \bmod n$

m^k is not a multiple of n because n is not a factor of m as $m < n$
Then, by Fermat's Little Theorem, $(m^k)^{n-1} \bmod n = 1$
Therefore, $m^{ed} \bmod n = m \bmod n$

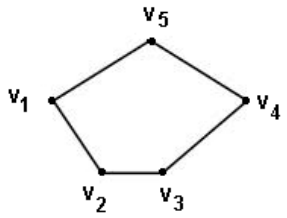
Hence, Bob can get back the original message m by calculating $c^d \bmod n$ where $c = m^e \bmod n$.

(b) No. Because n and e are public, so anyone can calculate d, which is the inverse of e, by extended GCD algorithm. Then, encrypted messages can be easily decrypted by anyone using the same decryption algorithm with the calculated d.

Problem 9: (15 Points)

In this question, n and k are integers such that $n \geq 3$ and $2 \leq k \leq n$.

Consider n points $v_1, ..., v_n$ on a 2D plane. If we connect v_i with v_{i+1} for $1 \leq i \leq n-1$ and connect v_n with v_1, then we get a *cycle* of length n. The following figure shows a cycle of length 5:



Suppose that we want to color the n vertices in a cycle of length n with k colors such that neighboring vertices get different colors. In how many ways can we do this? Explain your answer.

Solution of P9: The problem gives one way to color the vertices where neighboring vertices get different colors. Let T_n be the number of ways to do this. This is what we want to calculate.

Now consider a second way to color the vertices such that neighboring vertices get different colors **except that v_n is allowed to have the same color as v_1**. Let S_n the be number of ways to do this. Using the Product Principle, we get:

$$S_n = k(k-1)^{n-1}$$

A third way to color the vertices is such that neighboring vertices get different colors **except that v_n gets the same color as v_1**. Let R_n be the number to do this. We observe two facts:

$$T_n = S_n - R_n; \qquad R_n = T_{n-1}$$

So, we have

$$T_n = k(k-1)^{n-1} - T_{n-1}.$$

For the base case, we have

$$T_3 = k(k-1)(k-2).$$

Next, we solve the recurrence to get a closed-form formula for T_n. First notice that

$$T_n = (k-1)^n + (k-1)^{n-1} - T_{n-1}; \qquad T_3 = (k-1)^3 - (k-1).$$

Iterating the recurrence bottom up, we get

$$\begin{aligned} T_4 &= (k-1)^4 + (k-1) \\ T_5 &= (k-1)^5 - (k-1) \\ T_6 &= (k-1)^6 + (k-1) \\ T_7 &= (k-1)^7 - (k-1) \\ &\vdots \end{aligned}$$

So,

$$T_n = (k-1)^n + (-1)^n(k-1).$$

[SCRAP PAPER]

[SCRAP PAPER]

[SCRAP PAPER]